CYBER SECURITY TIPS (STAFFING EDITION)

In today's era of ever-increasing cyber-attacks, including malware, ransomware and many others, data security has never been more important for companies in the staffing and recruiting industry.

Considering the fact that the average cost of a data breach is $3.92 million (as of 2019) and damage related to cybercrime is projected to hit $6 trillion annually by 2021, it's absolutely mission critical to protect your business from cyber threats.

Sobering statistics like the ones above are precisely the reason why we put together a list of significant and practical tips to help staffing firms protect their businesses against cyber attacks.

1. SECURE EMAIL

Each day, the average American worker receives an astounding 121 emails. If you pair that with the fact that 90 percent of cyber attacks come via email, it's very important to secure your entire team's email. All it takes is one of those 121 emails to be a phishing scam that can cause mayhem to personal data. Here are a few basic tips to help improve email security:

- Never trust links (think twice before clicking)
- Examine URLs to make sure they're legitimate
- Double check email addresses to ensure it truly is coming from a trusted source
- Implement mandatory security training. This can take the form of hiring a consultant to come in and teach cyber security defense tactics or by simply putting together a Youtube Playlist of free training videos

2. TIGHTEN UP SECURITY

Did you know that most security breaches happen from within? People who work at staffing firms have access to a tremendous amount of personal information.

Think about the vast number of onboarding documents your employees have access to such as W4, I-9 and direct deposit forms. These all provide visibility into everything that translates into significant security risk.

Limit online access to only those who need it and be sure to log, monitor and report on the accessing of these files. On average, every employee has access to 17 million files. If your firm hasn't yet moved to paperless onboarding and document management, ensure these files are locked with limited employee access.

In addition, physically securing your business by installing security cameras, locks and alarm systems can go a long way in preventing would-be cyber attackers.

3. CHOOSE TECHNOLOGY PROVIDERS THAT TAKE SECURITY SERIOUSLY

The staffing industry relies heavily on a wide range of technology providers. From fully integrated staffing software to standalone solutions for background screening, WOTC, onboarding and compliances – firms could have anywhere from one to 20 systems that they are entering information into. While these tech companies can genuinely help firms unlock success, there is some risk, especially when it comes to cyber security.

When evaluating any third-party technology provider, be sure to ask if they are actively participating in cyber security best practices and see if they have a plan in case a breach were to occur. Here's an example of Avionté's security overview and standards for reference.

4. BACK UP YOUR DATA

Imagine for a moment the pure chaos that would unfold if your business suddenly lost all of your records from data corruption, natural disaster or ransomware. Picture processing payroll without anyone's information or recruiting talent with a blank ATS. Despite how unlikely a total data loss is these days, it's still absolutely critical to have at least one (preferably more) backups in place. In a nutshell, follow these best practices:

- Backup business data regularly (at least once every 24 hours or more)
- Create backups in the cloud or other reliable media sources
- Store data in more than one spot (local, cloud, etc.)

5. UPDATE YOUR SOFTWARE FREQUENTLY

Most SaaS solutions are automatically pushing updates in real time. If you are using an on-premise solution, anytime there's a software update available, update!

Updates contain important changes that will often improve the performance, stability and most importantly, the security of the applications.

From a simple app update to a major software update, be sure to update as often as you can.

6. INSTALL ANTI-MALWARE SOFTWARE

Anti-malware or anti-virus (often the same thing) put simply, protects your business against malicious software. In the old days, this software protected against computer viruses but with the evolution of cyber attacks, your anti-malware software should offer protection against (but not limited to):

- Spyware
- Adware
- Ransomware
- Phishing
- Spoofing
- Malvertising
- Exploits

7. USE A VPN

If you're not familiar, a VPN essentially hides your IP address and location, making you and your employees more anonymous on the internet. While not 100% safe, VPNs do increase security dramatically. There are a wide-variety of VPN providers that can offer protection for your internal and cloud-based resources.

8. HAVE A PLAN IF A BREACH DOES OCCUR

Assume a breach will happen. This will help your company not only have a plan for what to do if a breach occurs, it also allows your organization to be proactive in preventing attacks. Here are a few ideas of information to include in your plan:

- Create a response team of hand-picked individuals to address various issues (PR, HR, customer care, etc.)
- Develop plans for how to communicate a breach to your customers, partners and employees
- Identify a contact to assist with legal counsel
- Map out "to-dos" for your response team

9. UPDATE PASSWORDS FREQUENTLY

At a minimum, update your password every 90 days or 30 days for maximum security. Try to get in the habit of scheduling password reset days during the first of every month.

"On average, hackers attack 2,244 times a day"
- University of Maryland

Cyber security will continue to evolve and unfortunately, get more sophisticated over the years. Staying on top of cyber security best practices is your greatest chance of reducing your risk of an attack. If you need more tips, don't be afraid to check out Cyber Essentials by the Cybersecurity and Infrastructure Security Agency.